NEWS

Kontakt:

POWERLINK-OFFICE der EPSG
Kurfürstenstraße 112
10787 Berlin · Germany
Tel.: +49(0)30-85 08 85-29
Fax: +49(0)30-85 08 85-86
info@ethernet-powerlink.org
www.ethernet-powerlink.org

Sicherer Antriebscontroller deSDAC 3003 PLC für POWERLINK

Bild: Der Antriebscontroller deSDAC 3003 PLC mit POWERLINK-Interface

Mit dem deSDAC 3003 PLC bietet dresden elektronik ingenieurtechnik, Hersteller von Steuerungstechnik, einen Antriebscontroller für POWERLINK-Netzwerke, der neben der sicheren Antriebsregelung auch die sicherheitsgerichtete Datenverarbeitung für digitale und analoge Prozessperipherie erlaubt.

Der Controller, mit dem sich zwei Antriebe ansteuern lassen, arbeitet zweikanalig redundant mit gegenseitigem Vergleich. Er erfüllt die Sicherheitsanforderungen nach den Normen DIN EN 61508 (SIL 3) und DIN EN ISO 13849-1 (Kat. 4).
Optional steht das Gerät mit integrierter SPS auf Basis des KW-Software-Betriebssystems SafeOS zur Verfügung. Mit diesem sicheren SPS-Betriebssystem kann der Anwender sowohl komplexe Antriebsfunktionen als auch die nach dem PLCopen-Standard implementierten Sicherheitsbausteine nach IEC 61131 in seinem Applikationsprogramm verwenden. Als Engineering-Tool dient SAFEPROG. Der Antriebscontroller eignet sich zur Steuerung hoch-dynamischer Positionierantriebe, wie sie beispielsweise bei Werkzeugmaschinen, logistischen Anlagen und auch in der Bühnentechnik Anwendung finden. Gerade in Bereichen, in denen Fehlfunktionen in der Datenübertragung ein Gefahrenpotential für Mitarbeiter darstellen, kommt es auf eine tragfähige und umfassende Safety-Philosophie an. Das POWERLINK-Interface bildet hier eine ideale Grundlage für Netzwerke, in denen das sicherheitsgerichtete Protokoll POWERLINK Safety höchste Sicherheit nach SIL 3 für die Datenübertragung garantiert oder aber in denen das Echtzeitprotokoll POWERLINK sicheren Komponenten hohe Geschwindigkeiten und Bandbreiten zur Verfügung stellt. Ein integriertes Diagnose- und Bedienterminal bietet Unterstützung bei Inbetriebnahme und Diagnose durch die Anzeige von Peripheriezuständen und applikationsinternen Größen. Zwei ARM7-LPC2292 Mikrocontroller bilden die Plattform des Systems. Anwender können eigene Applikationen mit C/C++-Programmiersystemen erstellen.

WAGO: Feldbuskoppler für POWERLINK

Passend zum industrieerprobten Feldbussystem POWERLINK präsentiert WAGO mit dem I/O-SYSTEM 750 robuste Koppler auf Grundlage der POWERLINK-Spezifikation.

Fortsetzung auf Seite 2 →

NEWS

Kontakt:

POWERLINK-OFFICE der EPSG
Kurfürstenstraße 112
10787 Berlin · Germany
Tel.: +49(0)30-85 08 85-29
Fax: +49(0)30-85 08 85-86
info@ethernet-powerlink.org
www.ethernet-powerlink.org

Fortsetzung:

WAGO: Feldbuskoppler für POWERLINK

Bild: Feldbuskoppler I/O-System 750 von WAGO

Bis zu 64 E/A-Klemmen können an einem Gerät betrieben werden, mit Busverlängerung sind sogar 250 Klemmen möglich. Die Applikationsschnittstelle basiert auf dem CANopen-Kommunikationsprofil DS 301. Der Hauptvorteil von POWERLINK liegt darin, dass es einerseits auf Standardethernet basiert, andererseits aber auch höchste Anforderungen an Deterministik und Zykluszeit erfüllt. Dadurch ist dieses Protokoll für Anwendungen mit harten Echtzeitbedingungen, aber auch für den zeitlich definierten Transport großer Datenmengen prädestiniert. Zusätzlich verfügt es über eine flexible und ausgereifte CANopen-Anwendungsschnittstelle, wodurch der Anwender auf eine breite Basis vorhandener Geräte- und Anwendungsprofile zurückgreifen kann. Mit seinem breiten Spektrum von E/A-Klemmen bietet das WAGO I/O-SYSTEM 750 eine industrietaugliche Hardwarebasis für POWERLINK.

Die Fehlererkennungsmechanismen von POWERLINK Safety

Fehler in der Datenübertragung sind nie völlig zu beseitigen, müssen aber bei industriellen Anwendungen, wo sie zu Gefährdungen von Menschen und Maschinen führen können, unter allen Umständen rechtzeitig entdeckt werden. Es ist die Aufgabe von sicherheitsgerichteten Protokollen, fehlerbehaftete Datenpakete in jedem Fall zu erkennen, sie herauszufiltern oder gegebenenfalls den sicheren Zustand der Maschine oder Anlage einzuleiten.

Da POWERLINK Safety alle bekannten Fehler, die bei der Datenübertragung auftreten können, sicher erkennt, können mit dem Sicherheitsprotokoll auch unsichere Netzwerke für sicherheitsrelevante Anwendungen genutzt werden. Doch für welche Fehler muss das Protokoll im einzelnen gerüstet sein?

Fortsetzung auf Seite 3 →

NEWS

Kontakt:

POWERLINK-OFFICE der EPSG
Kurfürstenstraße 112
10787 Berlin · Germany
Tel.: +49(0)30-85 08 85-29
Fax: +49(0)30-85 08 85-86
info@ethernet-powerlink.org
www.ethernet-powerlink.org

Fortsetzung:

Die Fehlererkennungsmechanismen von POWERLINK Safety

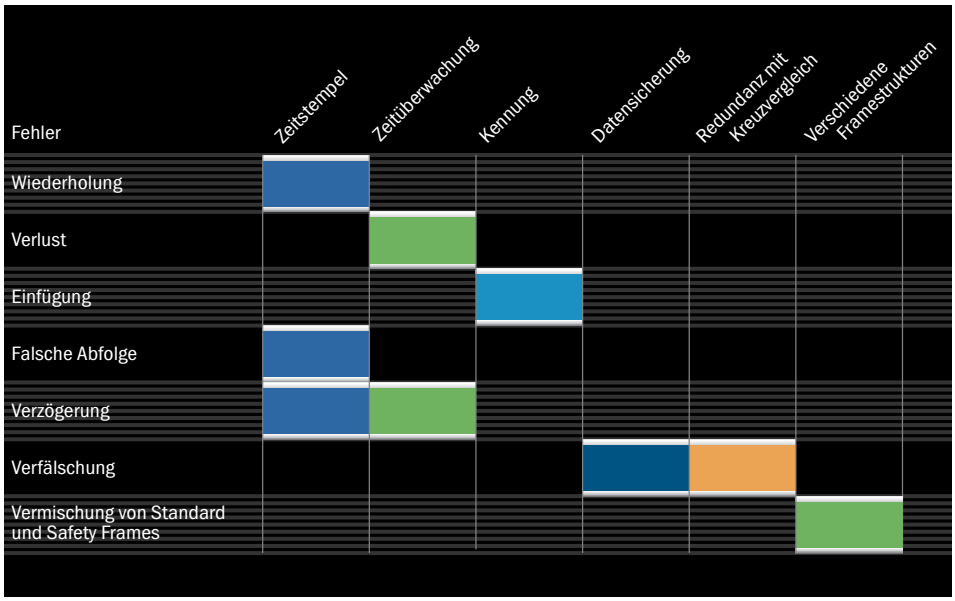

Bild 1: Die Fehlererkennungsmechanismen von POWERLINK Safety decken das gesamte Spektrum an Fehlern ab

Welche Fehler gibt es und warum?

Die Matrix in Bild 1 listet Fehler und die entsprechenden Verfahren auf, mit denen POWERLINK Safety diese Fehler erkennt. Die Fehler haben meist die folgenden Ursachen:

- Wiederholungen oder Verdopplungen von Datenpaketen können auftreten, wenn Netzwerke über mehrere Gateways miteinander verbunden sind. Im Fehlerfall übertragen zwei Gateways dieselben Daten, was zu einer Verdopplung führt.
- Datenverlust tritt ein, wenn ein Gateway Daten entweder gar nicht oder in ein falsches Netzwerk weiterleitet.
- Zu Einfügungen kann es kommen, wenn Datenpakete aufgrund ihrer Länge nur in mehreren Teilpaketen versendet werden können. Wenn Netzwerke über mehrere Gateways verbunden sind, kann es durch unterschiedliche Übermittlungswege zu Vertauschungen in der Reihenfolge der einzelnen Paketsegmente und zu Einfügungen von Segmenten in andere Pakete kommen.
- Gateways können bei hohem Datenaufkommen die Weiterleitung verzögern. Führt der Übertragungsweg auch hier über zwei Gateways, kann die chronologische Reihenfolge der Datenpakete durch die unterschiedlichen Verzögerungen durcheinandergeraten.
- Verfälschungen von Daten werden meist durch elektromagnetische Störeinflüsse verursacht, die ein „Kippen“ einzelner Bits oder die Zerstörungen ganzer Abschnitte zur Folge haben.
- Bei gleichzeitiger Nutzung des Netzes für Standard- und Safety-Daten ist es möglich, dass Standarddaten als sichere Daten wahrgenommen werden. Diese „Maskerade“ kann zu schweren Fehlfunktionen der Applikation führen.

Fortsetzung auf Seite 4 →

NEWS

Kontakt:

POWERLINK-OFFICE der EPSG
Kurfürstenstraße 112
10787 Berlin · Germany
Tel.: +49(0)30-85 08 85-29
Fax: +49(0)30-85 08 85-86
info@ethernet-powerlink.org
www.ethernet-powerlink.org

Fortsetzung:

Die Fehlererkennungsmechanismen von POWERLINK Safety

POWERLINK Safety, das für den Einsatz in Systemen mit SIL 3 geeignet ist, erreicht das hohe Maß an Sicherheit durch folgende Mechanismen:

Zeitstempel machen Datenpakete unverwechselbar

Zu den wichtigsten Mechanismen von POWERLINK Safety zählt der Zeitstempel. Der Sender prägt jedem Datenpaket die Zeit seiner Absendung und somit ein einzigartiges Merkmal auf. Dadurch werden Wiederholungen, vertauschte Reihenfolgen und Verzögerungen erkannt.

Zeitsynchronisation

Um Verzögerungen festzustellen, muss der Empfänger natürlich auch die zeitliche Abweichung zwischen der Uhr des Senders und der eigenen kennen. Das erfordert eine verlässliche Synchronisierung der Zeitgeber in den Microcontrollern von Sendern und Empfängern.

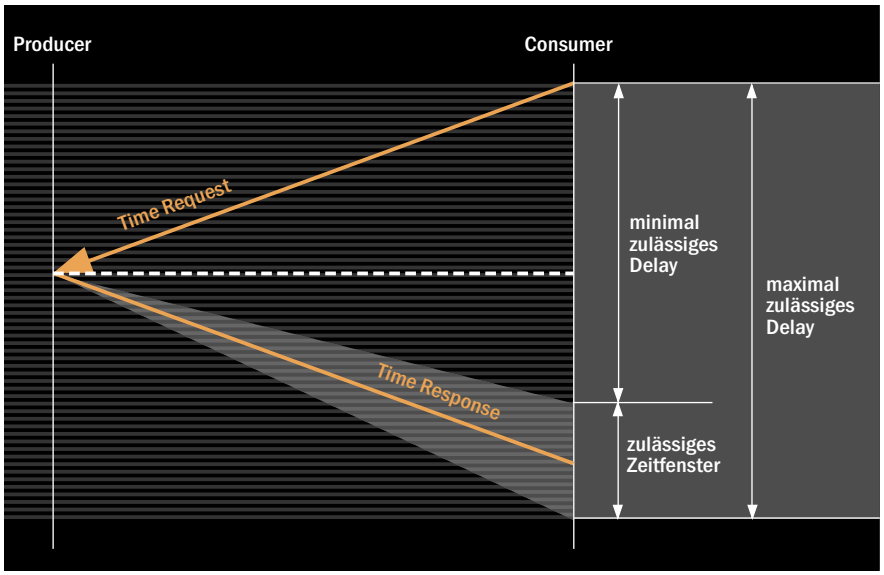

Bild 2: Schema der Zeitsynchronisation bei POWERLINK Safety.

Die Empfänger (Consumer) senden dafür in zyklischen Abständen eine Zeitanfrage TReq (Time Request) an die Producer, die darauf mit einer Zeitantwort TRes (Time Response) reagieren. Der Consumer verwertet nur Zeitantworten, die innerhalb eines realistisch definierten Antwort-Zeitraumes eintreffen.

Zeitüberwachung entdeckt unerlaubte Verzögerungen

Mit einer Zeitüberwachung registriert der Consumer auch dann, wenn der Producer gerade keine Prozessdaten zu senden hat, dass die Datenverbindung nicht unterbrochen ist und der Producer ordnungsgemäß funktioniert. Dazu senden Producer ständig „Lebenssignale“. Bleiben diese Signale aus, leitet der Consumer den sicheren Zustand ein.

Fortsetzung auf Seite 5 →

NEWS

Kontakt:

POWERLINK-OFFICE der EPSG
Kurfürstenstraße 112
10787 Berlin · Germany
Tel.: +49(0)30-85 08 85-29
Fax: +49(0)30-85 08 85-86
info@ethernet-powerlink.org
www.ethernet-powerlink.org

Fortsetzung:

Die Fehlererkennungsmechanismen von POWERLINK Safety

Eindeutige Kennung des Frames

Unzureichende Trennung von Netzwerken oder uneindeutige Kennzeichnung von Frames können Consumer „verleiten“, nicht für sie bestimmte Frames auszuwerten. POWERLINK Safety Frames verfügen über eine eindeutige Kennung des Frames, den Identifier, der Verwechslungen seitens des Empfängers ausschließt.

Datensicherung mit Prüfsummen

Das CRC-Verfahren (Cyclic Redundancy Check) dient dazu, Veränderungen oder Zerstörungen des Dateninhaltes zu erkennen. Aus jedem Datensatz wird mit einem Zahlenschlüssel eine Prüfsumme gebildet, die gemeinsam mit dem Schlüssel dem versendeten Datensatz angehängt wird. Die Prüfsumme codiert die Daten in unverwechselbarer Form. Der Empfänger errechnet aus dem Datensatz ebenfalls die Prüfsumme und vergleicht diese mit der gesendeten. Weichen die mitgesendete und die errechnete Prüfsumme voneinander ab, ignoriert der Empfänger die Nachricht.

Der POWERLINK Safety Frame

Außerdem verwendet POWERLINK Safety noch ein weiteres Verfahren der Datensicherung. Das Sicherheitsprotokoll verdoppelt den ursprünglich zu versendenden Frame, so dass ein POWERLINK Safety Frame aus zwei je mit eigener CRC-Summe gesicherten Unterframes mit identischen Nutzdaten besteht. Der Empfänger überprüft neben den Checksummen die Identität beider Unterframes.

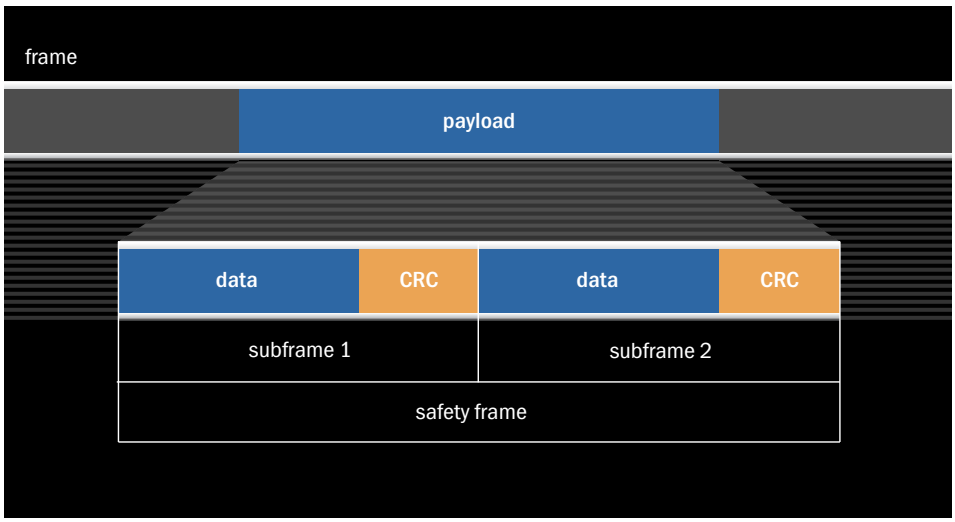

Bild 3: Das Safety Frame wird im Nutzdatenbereich eines Standardframes transportiert. Es besteht aus zwei identischen Subframes, die jeweils mit einer eigenen Prüfsumme gesichert werden

Keine Tarnung möglich

Den letzten Punkt in der Fehler-Liste bildet die Maskerade, also die „Tarnung“ von Standarddaten als sichere Daten. Das sehr spezielle Format des POWERLINK Safety Frames – zwei Unterframes mit jeweils eigener Prüfsumme – macht eine Verwechslung durch den Consumer extrem unwahrscheinlich.

NEWS

POWERLINK: Sicherheit durch Domänentrennung

In der Diskussion um Industrial Ethernet wird gelegentlich die Sorge geäußert, dass Ethernet-basierte Automationsnetzwerke die Sicherheit vor Angriffen nicht in ausreichendem Maß gewährleisten. Weil Industrial Ethernet den Vorteil durchgängiger Kommunikationsstrukturen von der Leit- bis zur Feldebene bietet, sei es, so lautet der Einwand, Angreifern auch prinzipiell möglich, über das Internet Manipulationen auf der Automationsebene durchzuführen.

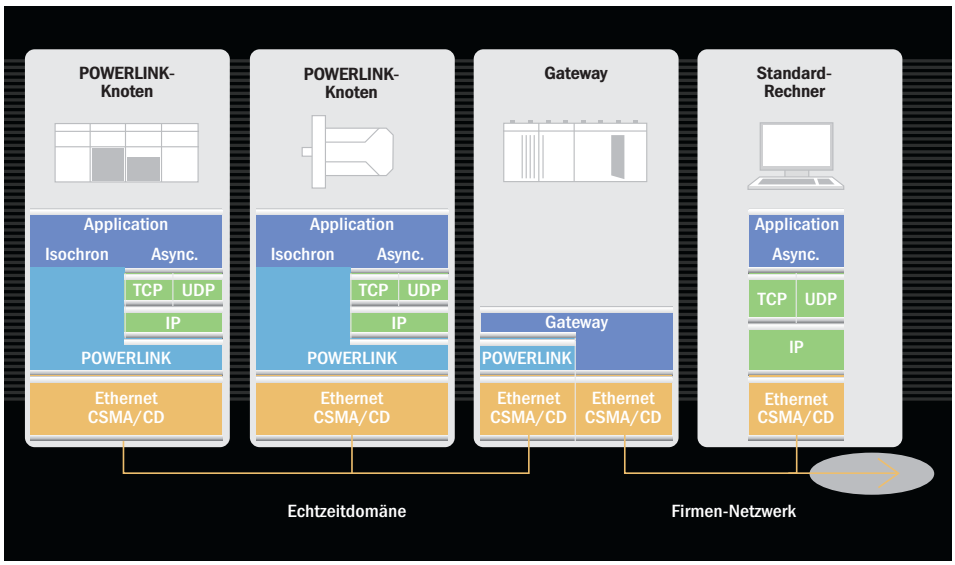

Bild: POWERLINK-Echtzeitdomänen werden durch Gateways strikt vom Netzwerk getrennt

Diese Sorge ist bei POWERLINK unbegründet. Eine Stärke des Kommunikationssystems liegt in seiner Fähigkeit, Standard Ethernet einzubinden, ohne dabei den hohen Sicherheitsstandard zu verletzen: POWERLINK-Echtzeitdomänen werden durch Gateways, die typischerweise direkt in die Steuerungen integriert sind, strikt von Nicht-Echtzeitdomänen getrennt. Jede Maschine oder Anlage, auf der POWERLINK läuft, bildet eine eigene Netzwerkdomäne, die nach außen nur über eine IP-Adresse repräsentiert wird. Die Gateways arbeiten dabei wie eine Firewall. Diese setzt die öffentliche IP-Adresse per Network Adress Translation (NAT) intern auf nichteinsehbare IP-Adressen der Knoten um. An den Gateways lassen sich zusätzlich individuell beliebige weitere Sicherheitsmaßnahmen und Filtervorschriften definieren und umsetzen.

Kontakt:

POWERLINK-OFFICE der EPSG
Kurfürstenstraße 112
10787 Berlin · Germany
Tel.: +49(0)30-85 08 85-29
Fax: +49(0)30-85 08 85-86
info@ethernet-powerlink.org
www.ethernet-powerlink.org

Impressum:
»POWERLINK Newsletter« ist ein Informationsdienst der EPSG – Ethernet POWERLINK Standardization Group, c/o Zürcher Hochschule für Angewandte Wissenschaften, InES, Technikumstrasse 22, 8401 Winterthur, Schweiz

Redaktion:
Rüdiger Eikmeier (Chefredakteur), Heiko Wittke – gii die Presse-Agentur GmbH, Immanuelkirchstr. 12, 10405 Berlin, Tel.: +49(0)30-53 89 65-0, Fax: +49(0)30-53 89 65-29